

RF: Hackemate

Alan Levy / Matias Perez

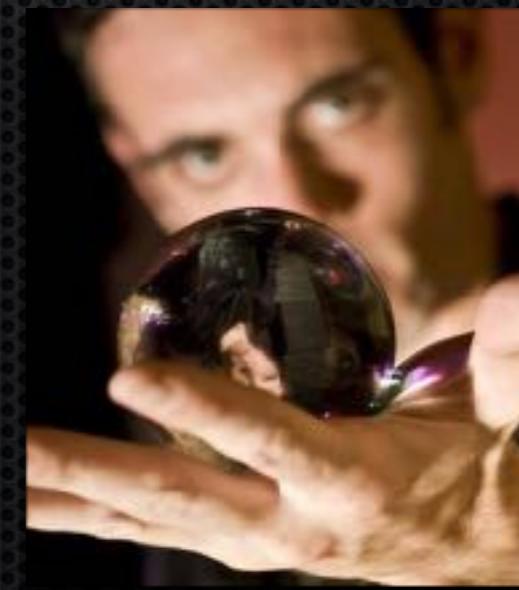


Marzo 2018 - Paraná - Entre Ríos
#ParanaConf

Who We Are

Alan Levy

- Information Security Consultant at Cinta Infinita.
- Ilusionista.



Matias Perez

- Emprendedor
- Apasionado por la tecnología y la seguridad informática.



Agenda

- Motivación
- Que es RF?
- RF: Por Hardware y SDR
 - Hardware y Software utilizado en esta charla
- Ataques
 - Demos
- Conclusiones
 - Medidas de mitigación



Motivación

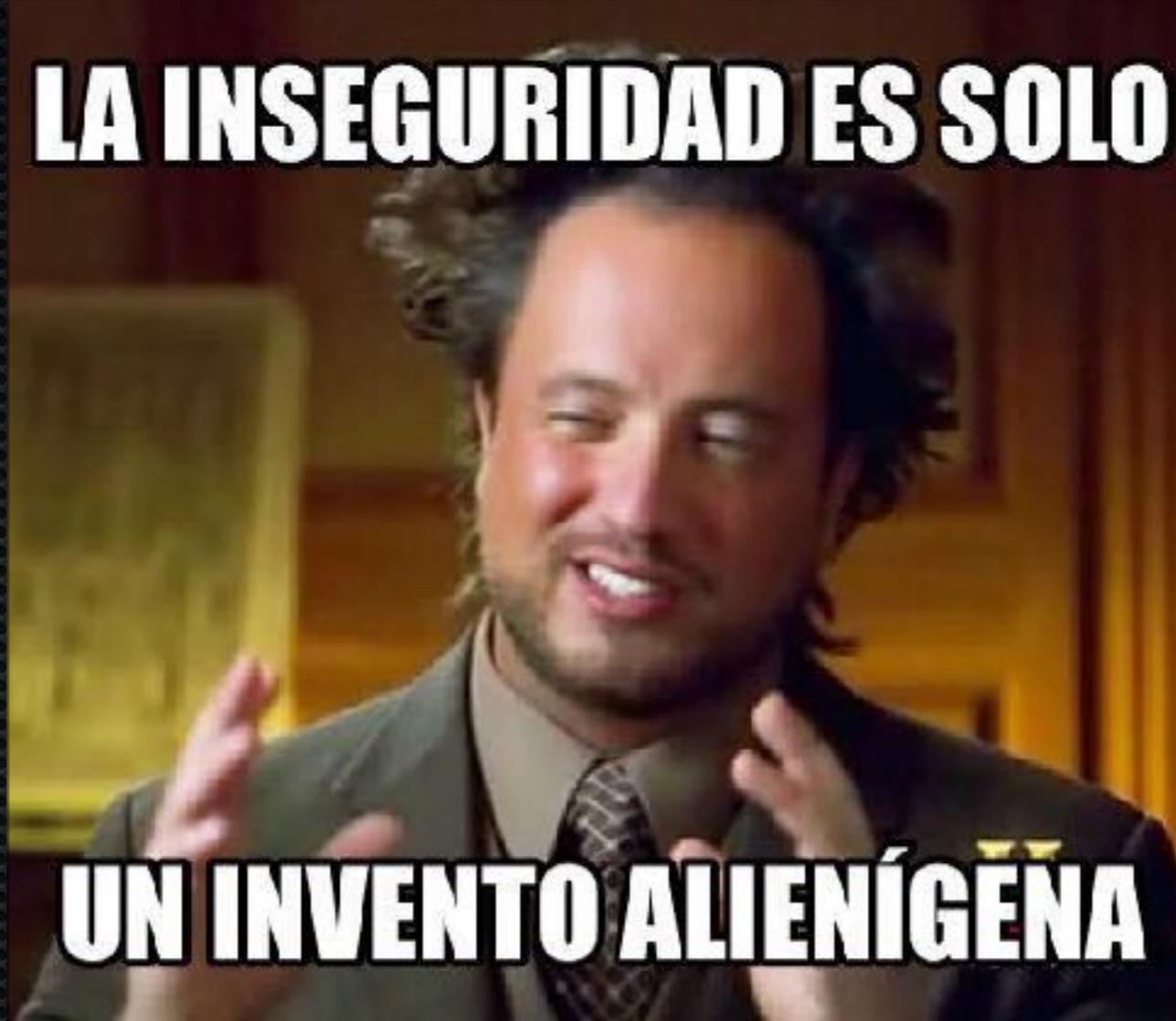
Motivación



Motivación

LA INSEGURIDAD ES SOLO

UN INVENTO ALIENÍGENA



Disclaimer

Disclaimer



Disclaimer



Es necesario aclarar que NO somos radioaficionados, ni somos experto en radio frecuencia. Además, queremos destacar que ninguno de los ataques que mostraremos durante la charla fueron descubierto por nosotros, son investigaciones de otras personas que nosotros hemos tomado, estudiado y reproducido. Esperamos aportar desde la concientización.

Disclaimer



Es necesario aclarar que NO somos radioaficionados, ni somos experto en radio frecuencia. Además, queremos destacar que ninguno de los ataques que mostraremos durante la charla fueron descubierto por nosotros, son investigaciones de otras personas que nosotros hemos tomado, estudiado y reproducido. Esperamos aportar desde la concientización.

Por último y no menos importante, decir que, ningún vehículo, garaje, alarma, ni máquina de ningún tipo salieron lastimadas durante el rodaje de los videos demos que se verán a continuación.

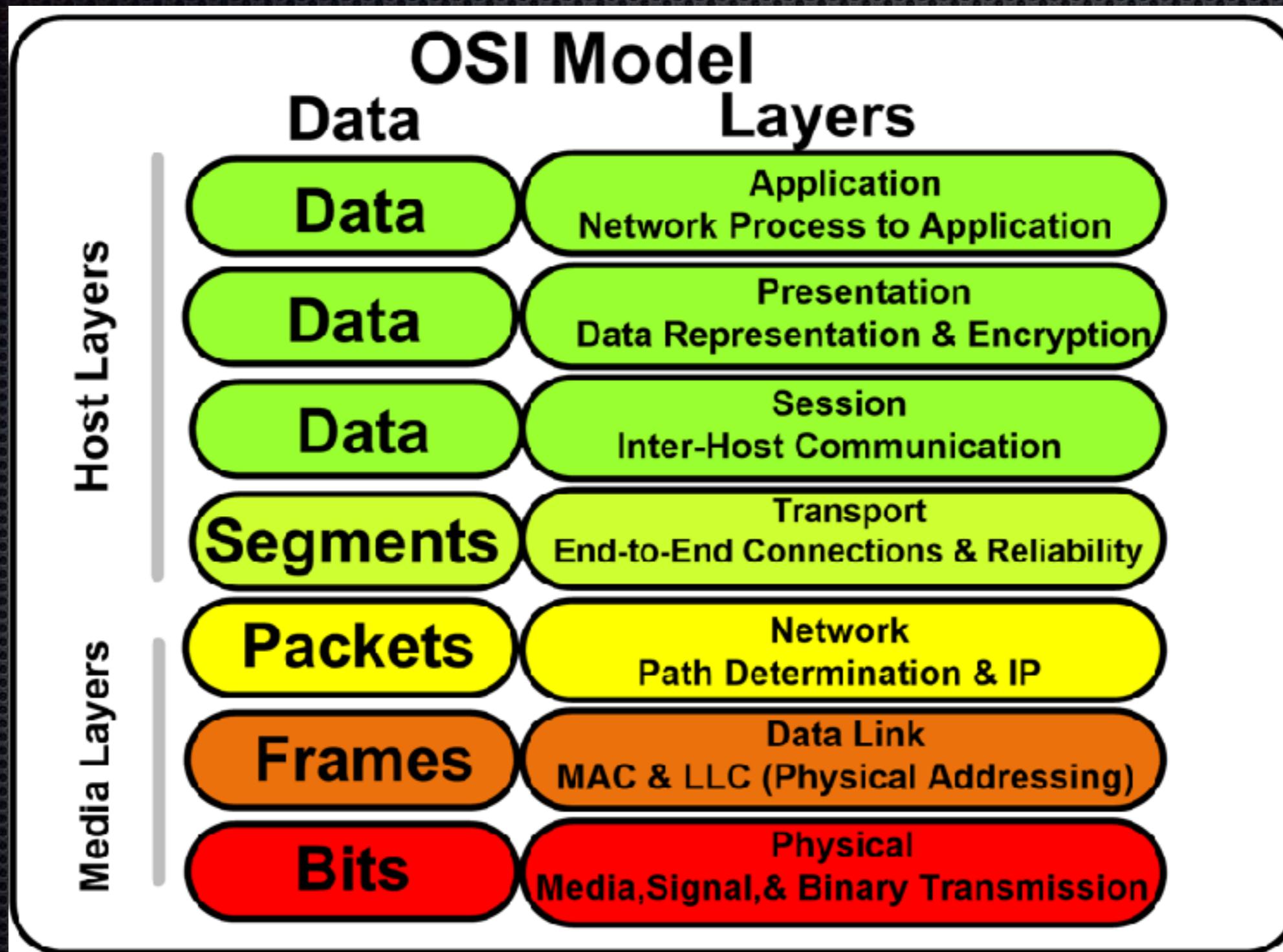
Que es RF?

Transmisión de energía mediante ondas electromagnéticas (entre 3Hz y 300GHz)

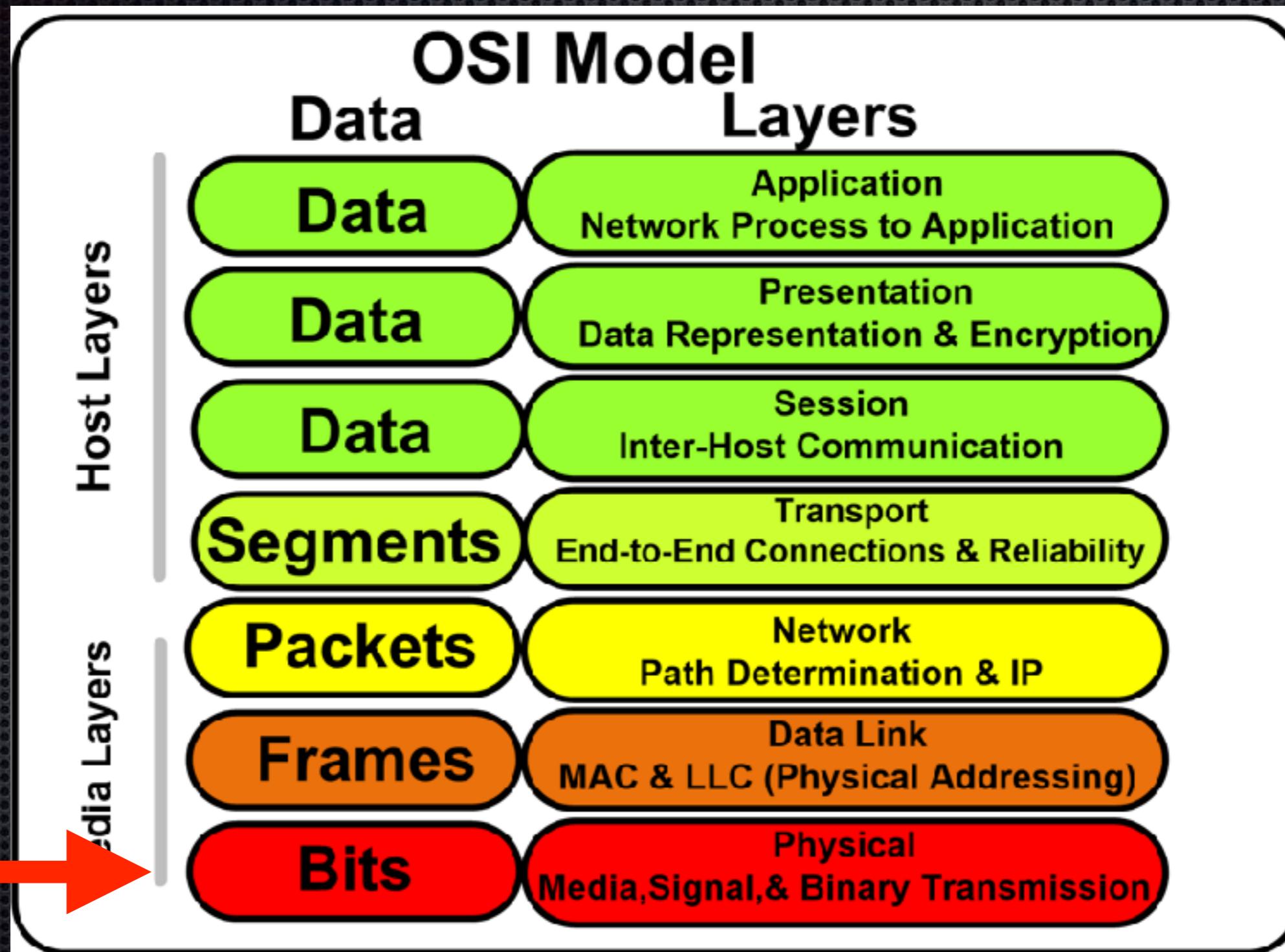
Capa Física del Modelo OSI.

Utilizado en diferentes tecnologías (comunes y no tan comunes)

Que es RF?



Que es RF?



Que es RF?

Transmisión de energía mediante ondas electromagnéticas (entre 3Hz y 300GHz)

Capa Física del Modelo OSI.

Diferentes tipos de señales.

Utilizado en diferentes tecnologías (comunes y no tan comunes)

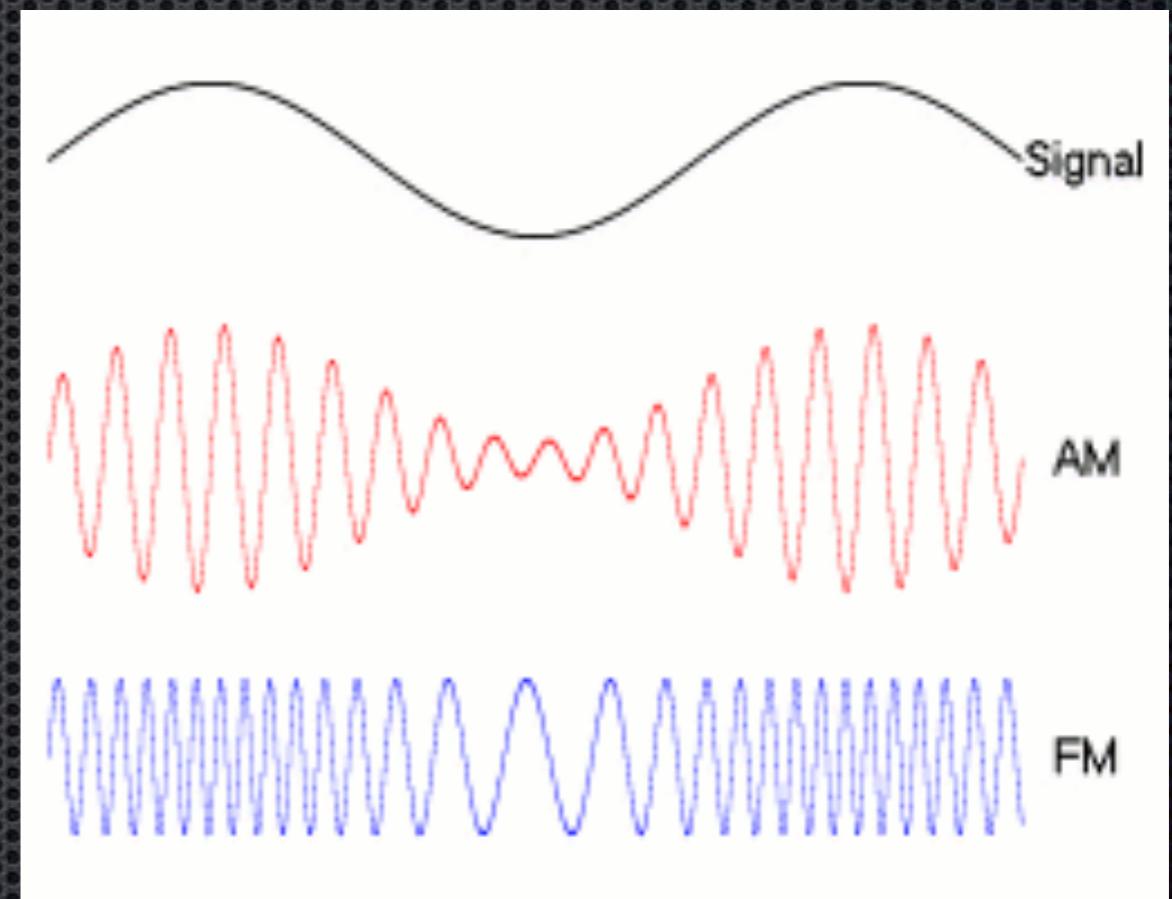
Que es RF?

Transmisión de energía mediante ondas electromagnéticas (entre 3Hz y 300GHz)

Capa Física del Modelo OSI.

Diferentes tipos de señales.

Utilizado en diferentes tecnologías (comunes y no tan comunes)



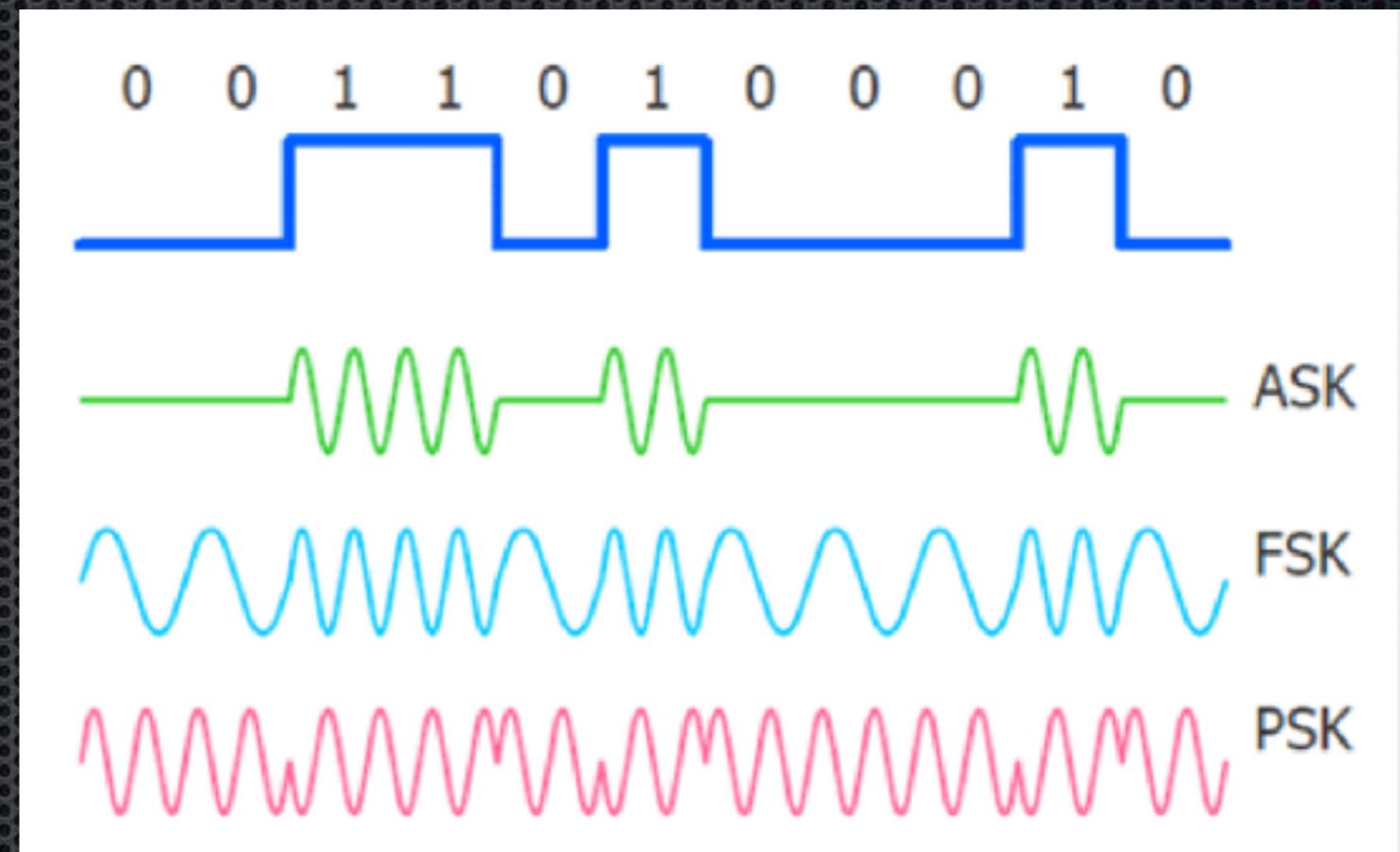
Que es RF?

Transmisión de energía mediante ondas electromagnéticas (entre 3Hz y 300GHz)

Capa Física del Modelo OSI.

Diferentes tipos de señales.

Utilizado en diferentes tecnologías (comunes y no tan comunes)

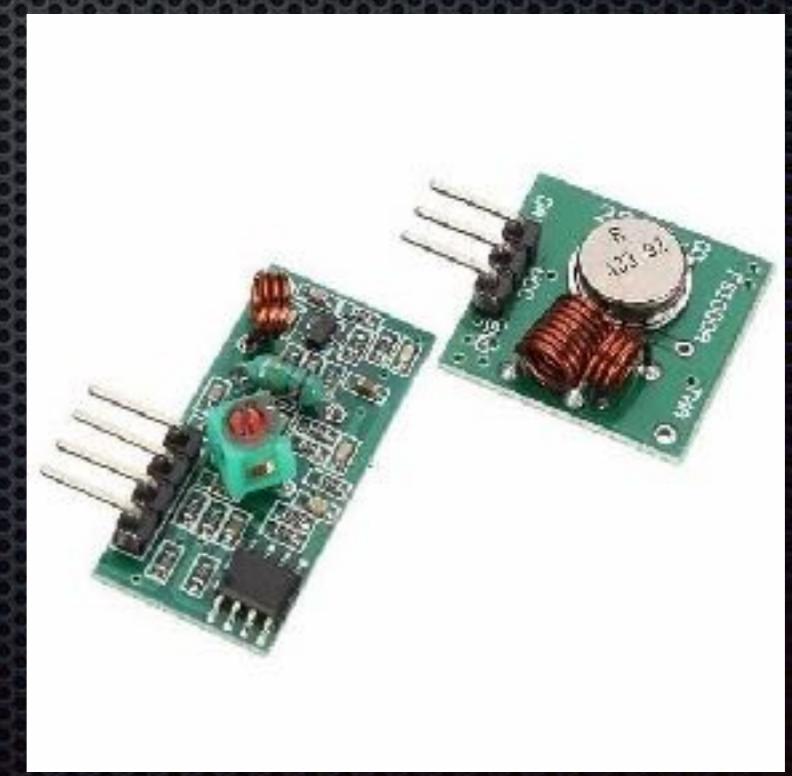
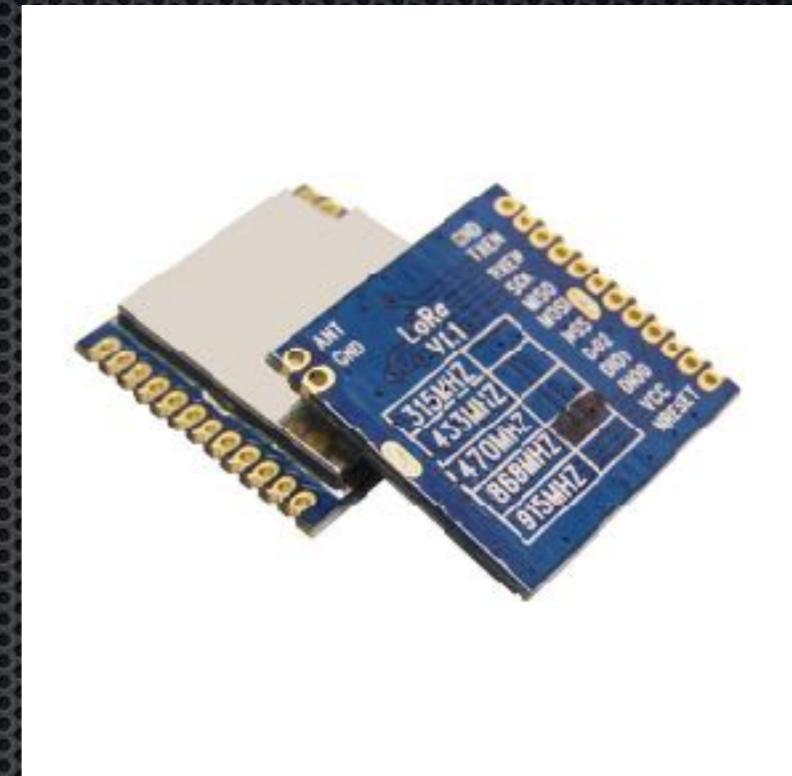


RF: Hardware

Viene escrita la frecuencia en la cual trabaja entre otras cosas en el propio hardware y no se puede modificar.

(Ej. 433Mhz, 315Mhz, etc.)

Por ejemplo módulos RF para Arduino.



RF: Hardware SDR

RF: Hardware SDR

SDR: Radio Definida por Software.

Un sistema de radio comunicación donde los componentes típicamente implementados en el hardware (mixers, filtros, moduladores, amplificadores, etc) en su lugar son implementados por software.

SDR proporciona un front-end de radio reconfigurable, donde se podrá cambiar por ejemplo, la frecuencia central ademas de muchas otras cosas que un hardware no permite.

En lugar de tener un hardware para cada protocolo (Bluetooth, Wifi, etc) se tiene un SDR y simplemente se cambia el software en la computadora para “hablar” estos diferentes protocolos pero siempre utilizando el mismo hardware.

RF: Hardware SDR



RTL_SDR

\$30

13 - 1864 MHz* (Receive Only)



HackRF One

\$300

10 MHz to 6 GHz (Transmit & Receive)



Ellisys Explorer 400-STD-LE

\$30,000

Capture & decode all Bluetooth channels at once



Ubertooth One

\$130

2.4GHz (Transmit & Receive)



Yardstick One

\$100

< 1 GHz (Transmit & Receive)

IM Me (OpenSesame)



CrazyRadio PA (or any nRF24LU1+ chip)

\$30

2.4 GHz (Transmit & Receive)

MouseJack

RF: Software para SDR

- GnuRadio
- Distros Linux “SDR Ready”
(Ej.: Sky Wave Linux)
- GQRX



Hardware utilizado para las demos

- ❖ HackRF One
- ❖ Raspberry PI
- ❖ Baofeng uv-5r
- ❖ Dispositivos RF varios
- ❖ RTL SDR (2832U)
- ❖ Maquina de Humo ;-)



HackRF One (El protagonista)

- Open Source
- Half Duplex
- Rango 1MHz a 6GHz
- 20M Samples por seg.
- 300 Dólares



Software utilizado para las demos

- GnuRadio
- GQRX
- Linux & MacOS
- Audacity
- Inspectrum
- Paint ;-)

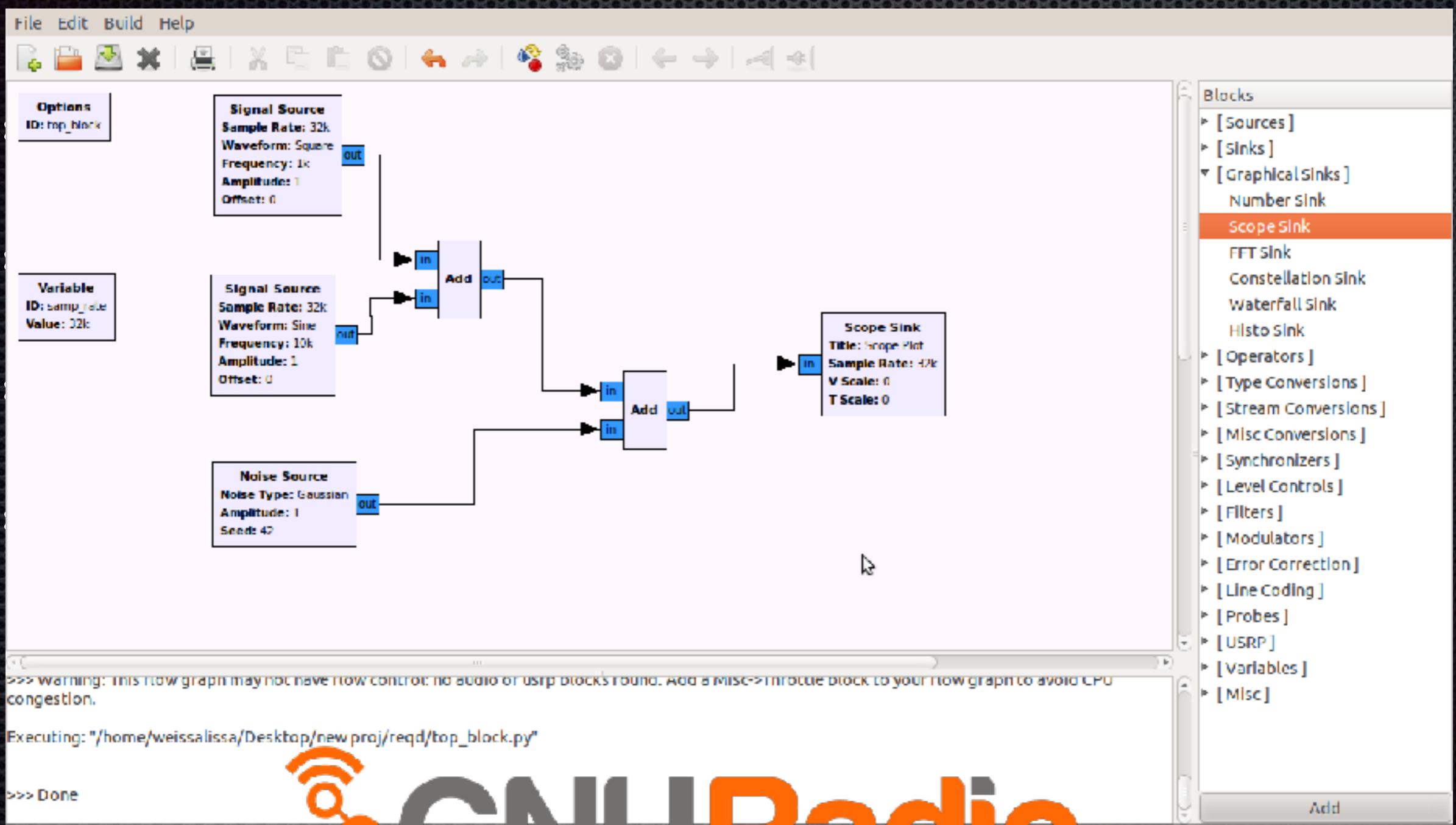


GNURadio (El protagonista)

- Open Source
- Programación por “bloques” o Python
- Compatible con HackRF y otros hardware low cost
- Muchos ejemplos en la Web



GNURadio (El protagonista)



Jamming



Jamming



Jamming







Jamming: Emitir una interferencia para impedir la transmisión de otra señal de radio a una determinada frecuencia.

Replay Attack



El replay attack consiste en escuchar la comunicación entre el emisor y el receptor, capturar ese paquete de datos, y luego reenviarlo sin ninguna modificación.

Primero se busca la frecuencia en la que trabaja el dispositivo, desarmando el dispositivo para ver si la frecuencia esta indicada en alguna parte o bien buscando el ID de la FCC (La Comisión Federal de Comunicaciones) <https://www.fcc.gov>.

Comúnmente las frecuencias mas utilizadas son 433MHz para Europa y 315MHz en USA.

Una vez identificada la frecuencia podremos utilizar el analizador de espectros GQRX para asegurarnos que la frecuencia indicada es la correcta.

Este ataque es posible siempre y cuando los datos que se manden al receptor no varíen (por ejemplo, mediante el uso de Rolling Codes).

Replay Attack



Replay Attack



Replay Attack



Replay Attack



Replay Attack



Replay Attack



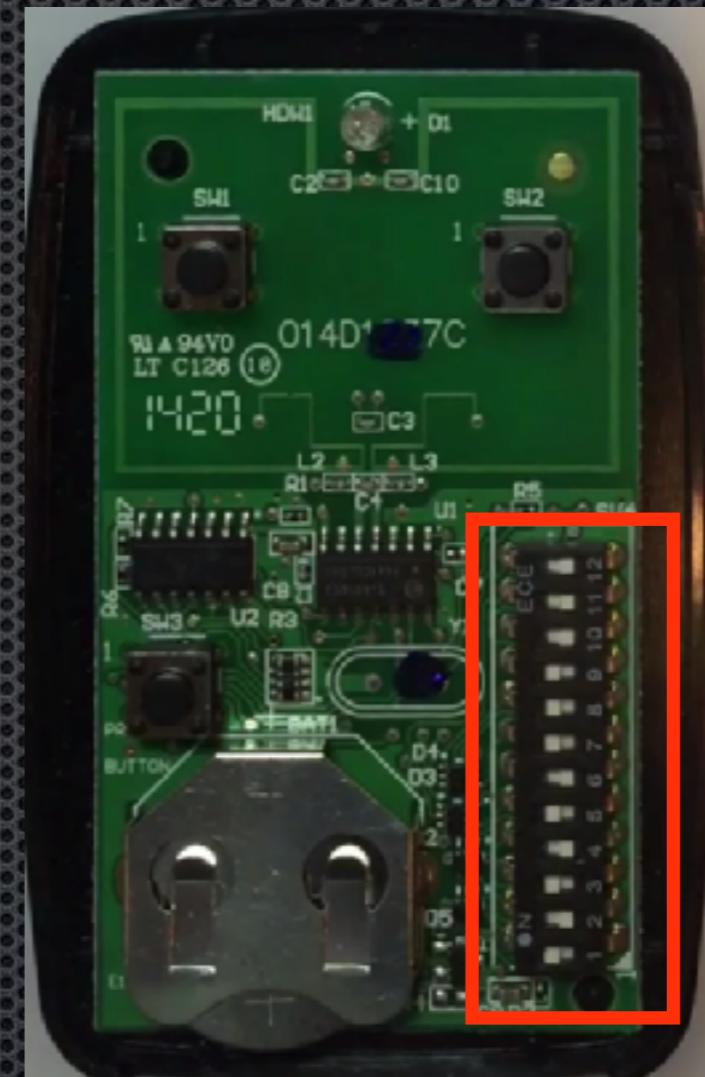
Fuerza Bruta o... “Abrete Sésamo”

Fuerza Bruta o... “Abrete Sésamo”



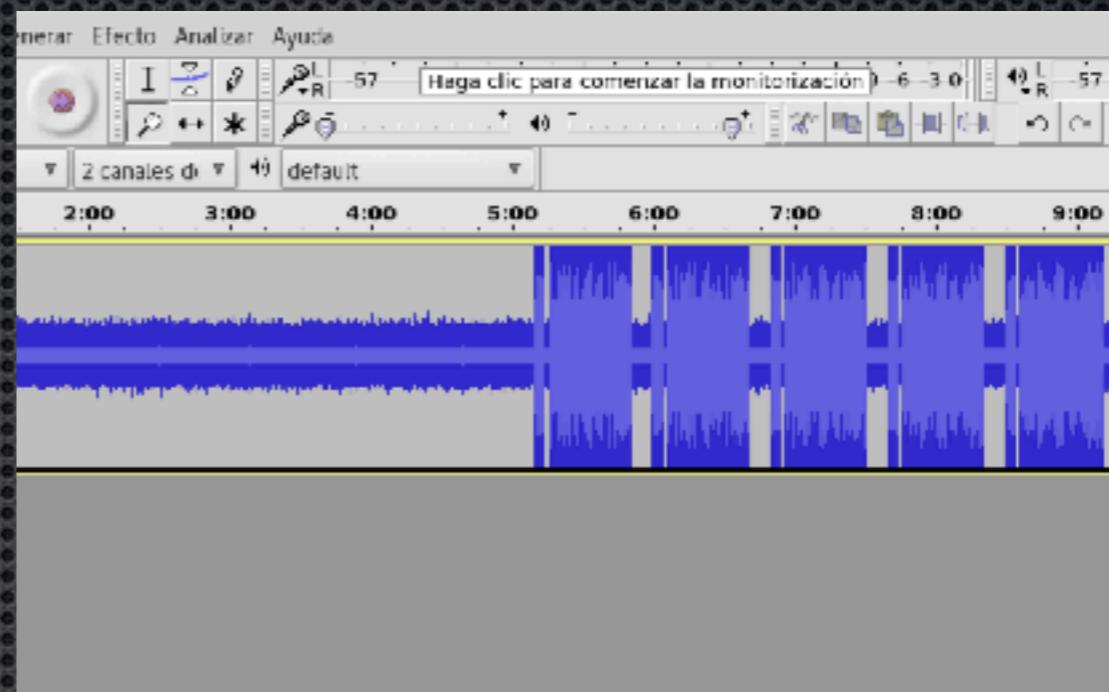
Fuerza Bruta Portón Garaje

- 8 - 12 bit por código
- 2ms por bit + 2ms delay
- 5 señales iguales
- $$\begin{aligned} & ((2^{**} 12)^{*} 12) + ((2^{**} 11)^{*} 11) \\ & + ((2^{**} 10)^{*} 10) + ((2^{**} 9)^{*} 9) \\ & + ((2^{**} 8)^{*} 8) = 88576 \text{ bits} \end{aligned}$$
- $$88576 \text{ bits} * (2\text{ms signal} + 2\text{ms delay}) * 5 \text{ transmisiones} = 1771520\text{ms} = 1771\text{seg} = \mathbf{29.5 \text{ minutos}}$$



Fuerza Bruta Portón Garaje

- 8 - 12 bit por código
- 2ms por bit + 2ms delay
- 5 señales iguales
- $((2^{12} * 12) + (2^{11} * 11) + (2^{10} * 10) + (2^9 * 9)) * ((2^{12} * 12) + (2^{11} * 11) + (2^{10} * 10) + (2^9 * 9)) = 88576 \text{ bits}$
- $88576 \text{ bits} * (2\text{ms signal} + 2\text{ms delay}) * 5 \text{ transmisiones} = 1771520\text{ms} = 1771\text{seg} = \mathbf{29.5 \text{ minutos}}$

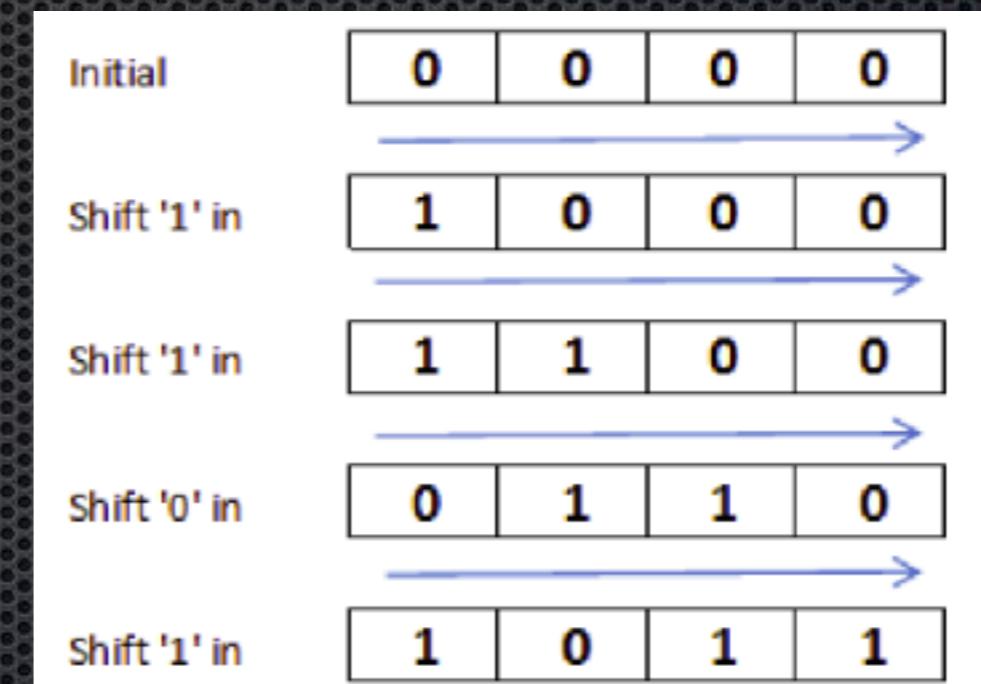


Fuerza Bruta Portón Garaje

- Si se eliminan 4 señales y solo se envía 1: 1771 seg/5
 $= 352.2 = 6 \text{ minutos}$
- Finalmente, al quitar los tiempos de espera simplemente se envía el código entero sin los wait time. Eso hace que se reduzca a **3 minutos.**
- Como el garaje sabe cuando el código comienza y cuando termina? Quizás una Bit Shift Register **(Registros de Desplazamiento)**

Fuerza Bruta Portón Garaje

- Finalmente, al quitar los tiempos de espera simplemente se envía el código entero sin los wait time. Eso hace que se reduzca a **3 minutos**.
- ¿Como el garaje sabe cuando el código comienza y cuando termina?
Quizás usa Bit Shift Register?



(Registros de Desplazamiento)

Fuerza Bruta Portón Garaje

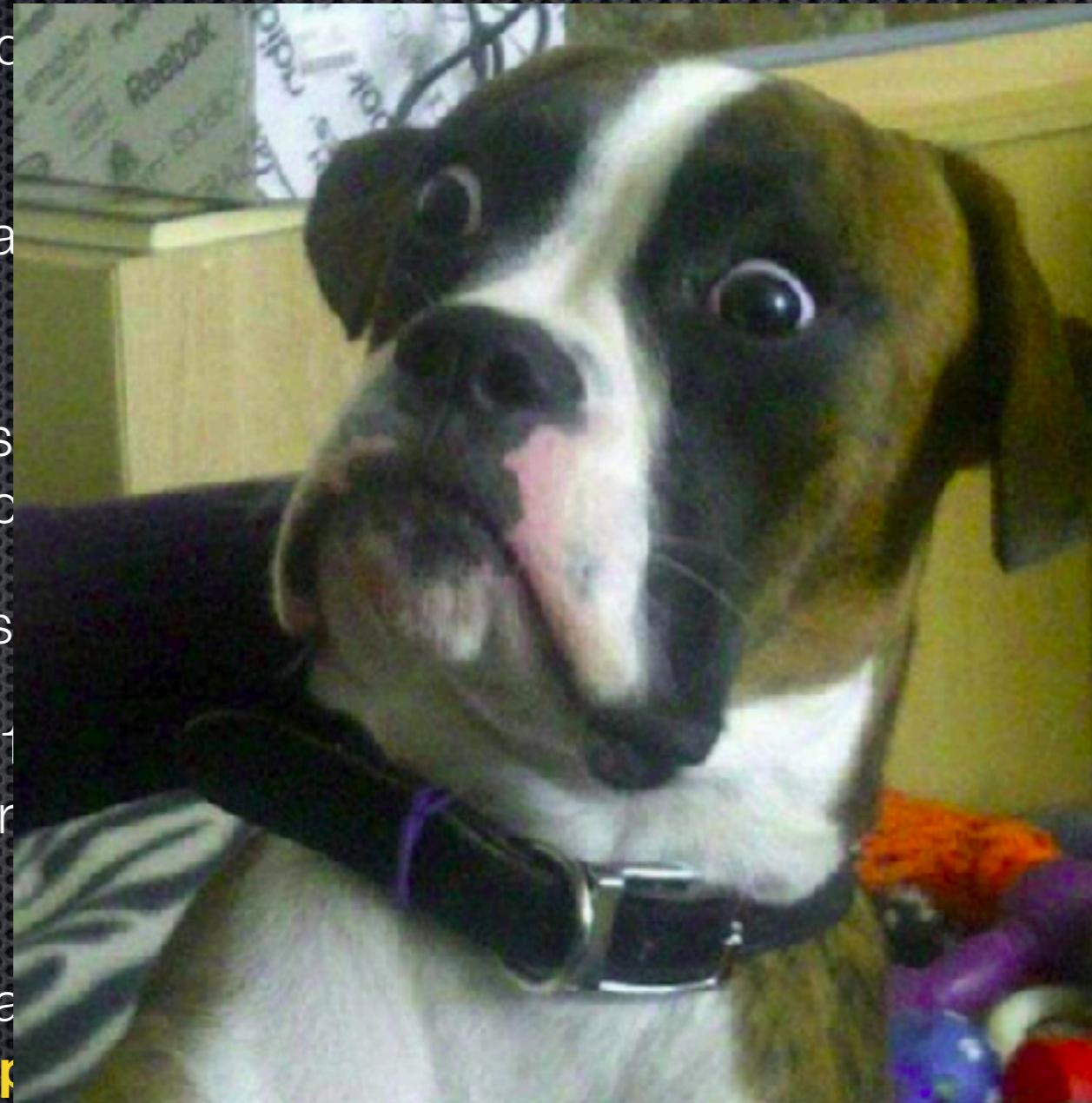
- Comúnmente utilizado cuando se leen bits del aire, se almacenan en un **Registros de Desplazamiento**
- Usando la secuencia de **De Bruijn**, es la manera mas eficaz “bruteforcear” esto:

Supongamos que el pin es 111111000000. Si el garaje usa un registro de desplazamiento y nosotros enviamos 13 bits "**0**111111000000", el garaje primero probará: 011111100000 (incorrecto).

- Vuelve a verificar la secuencia de códigos completa a medida que llega cada bit individual.
- Luego de probar **0**11111100000 (incorrecto) (elimina el primer bit y trae el próximo) 11111100000**0** (correcto! se abre.) Ademas se prueban a la vez los códigos de 11, 10, 9 y 8 bits también!
- El tiempo para probar cada posibilidad de 8 a 12 bits: $((2^{**} 12) + 11) * 4\text{ms} / 2 = 8214\text{ms}$ = **8.214 segundos para abrir cualquier garaje!**

Fuerza Bruta Portón Garaje

- Comúnmente utilizado para el **Desplazamiento**
- Usando la secuencia de bits:
Supongamos que el ladrón y nosotros enviamos el código 011111100000 (incorrecto)
- Vuelve a verificar la secuencia de bits:
Luego de probar 011111100000, el ladrón intentará los siguientes códigos de 11, 10, 9 y 8 bits también!
- El tiempo para probar 11 bits = **8.214 segundos** ($11 \times 4ms / 2 = 8.214ms$)



n un **Registros de Entrada/Salida** (RSI) se "forcear" esto:
el ladrón intentará el primer bit de desplazamiento y si no lo robará:
y el ladrón intentará el segundo bit individual.
y así sucesivamente. Si el ladrón trae el próximo bit de la secuencia, el ladrón intentará los siguientes códigos de 11, 10, 9 y 8 bits también!

1) * 4ms / 2 = 8214ms

Rolling Code “RollJam Attack”

Rolling Code “RollJam Attack”



Rolling Code “RollJam Attack”



Rolling Code “RollJam Attack”

- Se jamea la frecuencia de la alarma. El conductor quiere abrir su auto (manda la primer señal) y el auto no responde. El atacante captura esa señal que envió el conductor (entonces ya tiene un rolling code en su poder).
- Ahora, como el auto no se abrió, el conductor pulsará nuevamente el control de la alarma. El atacante sigue jameando, pero esta vez, manda al auto (haciendo un replay attack) la primer señal capturada mientras **guarda la segunda**.
- De esta manera el auto se abre y el atacante ahora posee un código (rolling code) válido para ser usado.

Otros ejemplos de ataques

- Sniffing de teclados wireless
- Captura de imágenes de monitores
- Denegaciones de Servicio
- Etc, etc, etc...



Otros ejemplos de ataques

Y el cerebro humano? Emite ondas electromagnéticas? SI!

Otros ejemplos de ataques

Y el cerebro humano? Emite ondas electromagnéticas? Si!

No has accedido | [Discusión](#) | [Contribuciones](#) | [Crear una cuenta](#)

[Artículo](#) [Discusión](#) Leer Editar Ver historial Buscar en Wikipedia



WIKIPEDIA
La enciclopedia libre

[Portada](#) [Portal de la comunidad](#) [Actualidad](#) [Cambios recientes](#) [Páginas nuevas](#) [Página aleatoria](#) [Ayuda](#) [Donaciones](#) [Notificar un error](#) [Imprimir/exportar](#) [Crear un libro](#)

Onda cerebral

Onda cerebral es la actividad eléctrica producida por el [cerebro](#). Estas ondas pueden ser detectadas mediante el [electroencefalógrafo](#) y se clasifican en:

- [ondas delta](#) (1 a 3 Hz)
- [ondas theta](#) (3,1 a 7,9 Hz)
- [ondas alpha o ritmo mu](#) (8 a 13 Hz)
- [ondas beta](#) (14 a 29 Hz)
- [ondas gamma](#) (30 a 100 Hz)

Véase también [editar]

- [Potenciales evocados](#)
- [P300](#)

Otros ejemplos de ataques

Otros ejemplos de ataques

Y si pudiéramos por ejemplo... Jampear el cerebro?

Otros ejemplos de ataques

Y si pudiéramos por ejemplo... Jampear el cerebro?

Ah, eso ya está inventado...

Otros ejemplos de ataques



Medidas de Mitigación?

Medidas de Mitigación?



Medidas de Mitigación?

Medidas de Mitigación?

Cómo podemos mejorar un poco todo este lío?

- No usar códigos cortos.
- Requerir una clave de preámbulo / sincronización para el comienzo de cada key.
- Usar rolling codes.

Medidas de Mitigación?

Cómo podemos mejorar un poco todo este lío?

- No usar códigos cortos.
- Requerir una clave de preámbulo / sincronización para el comienzo de cada key.
- Usar rolling codes.

Mejoras posibles para la implementación de Rolling Codes:

- Cifrar la acción del botón.
- Utilizar algún challenge/response.
- Tiempo de vigencia del código (actualmente no tienen timeout)
- Una “ventana” más pequeña para escuchar la señal.
- Que otra se te ocurre?

Medidas de Mitigación?

Cómo podemos mejorar un poco todo este lío?

- No usar códigos cortos.
- Requerir una clave de preámbulo / sincronización para el comienzo de cada key.
- Usar rolling codes.

Mejoras posibles para la implementación de Rolling Codes:

- Cifrar la acción del botón.
- Utilizar algún challenge/response.
- Tiempo de vigencia del código (actualmente no tienen timeout)
- Una “ventana” más pequeña para escuchar la señal.
- Que otra se te ocurre?

“Conocer la debilidad de los dispositivos es la primer protección”

Conclusiones

Conclusiones

En Argentina el ataque más usado según un estudio realizado es el de “fuerza bruta”

Conclusiones



Conclusiones

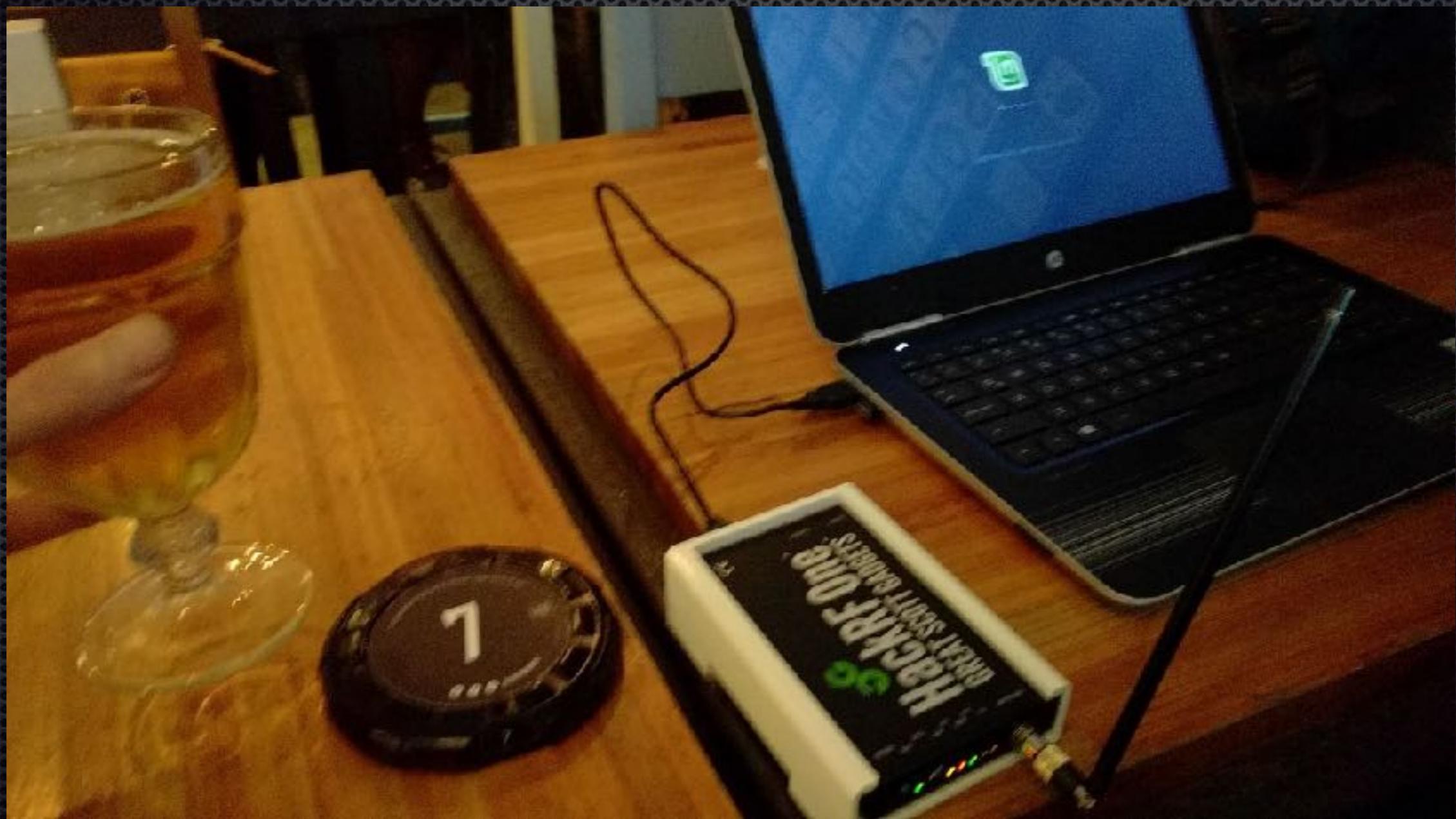


Conclusiones

Hacer research puede ser una tarea muy sacrificada...

Conclusiones

Hacer research puede ser una tarea muy sacrificada...



Muchas Gracias !!!

Contacto:

@soyelmago - alan@cintainfinita.com.ar

@pimgux - pimgux@gmail.com

Bibliografias, Slides, Videos Demos (y otros), códigos y más en:



/ThePimgux /MindTheGapSecurity @mtg_security